LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Securing an Apache Web Server on Amazon Cloud Platform

Abrahams, Oluwafemi J.

2016 Leppavaara

Laurea University of Applied Sciences
Leppavaara

Securing an Apache Web Server on Amazon Cloud Platform

Oluwafemi J. Abrahams
Degree Programme in Business IT
Bachelor's Thesis
December, 2016

Laurea University of Applied Sciences
Degree Programme in Business Information Technology
Bachelor's Thesis

Abstract

Name(s) Oluwafemi Johnson Abrahams

Securing an Apache Web Server on Amazon Cloud Platform

Year 2016 Pages

Most users of cloud computing services have security concerns when deploying their applications on a cloud infrastructure. This is so much more so for companies, big or small, who have chosen the Apache web server for hosting their applications in the cloud. While cloud service providers are increasingly augmenting security features available to their customers, the onus of using these security mechanisms lies with the customers. Striking a balance between the security technologies as well as the policies and best practices or non-technical factors are paramount to augmenting the security stance of a cloud-based web server and the supporting infrastructure. This thesis is an investigation into the technical and non-technical factors adversely affecting Softetape's customers.

Keywords
Cloud computing, web server, Iaas, Paas, SaaS, apache, amazon, IAM, security framework

Table of contents

1 Introduction

According to w3techs.com and netcraft.com web servers' usage statistics, Apache web server has the lion share in the HTTP server market. This also makes it the most targeted web server by cyber attackers.

1.1 Company Profile

Softetape Technologies Limited is a leading ICT and telecommunication services provider in West Africa and has branches or joint venture in virtually all major West African cities. The company headquarter is based in Lagos, Nigeria. The company has into five division namely:

- Services and Products
- Corporate Trainings
- Cloud Computing Services
- Network Services
- Power Solutions

This project was commission by Softetape Ltd. on behalf of its cloud computing services unit to identify and address some of the security problems the clients of the unit have been experiencing lately as regards the security of their web servers in the cloud. These clients consist of small startups, independent technology consultants as well as other small and medium scale enterprise.

1.2 Objectives and Scope

This thesis does not intend to solve or give random recommendations to mitigate all the issues of Apache web server security in the cloud but to research, identify and proffer solutions accordingly to those security issues (technical or otherwise) affecting the aforementioned clients. While the author will strive to report his findings accurately, all data or information that could jeopardy any of the clients' server security will not make it to the publicly viewable version of the thesis. Other aims of this thesis are as follows

- identify technical threats to the clients' web server in the cloud and proffer plausible solutions
- pinpoint non-technical factors that are affecting the clients' web server security posture
- choose an actionable security framework(s) that will increase the clients web server security stance when followed
- create and document a simply reference implementation model for new startup wanting to use Amazon AWS.

1.3 Assumptions

During the course of this thesis, the following presumptions are made:

- the cloud-based servers are running Linux Operating systems and that the clients or their delegates are comfortable using them
- the development computer is a MacBook or a PC running Linux operating system
- all server operating systems have been well configured and harden to withstand the worst attack

2 Research Methodology

Since primary goal of this inquest is to have insights to the root causes of security breaches rather than gather analyzable data, the qualitative approach of research will be used (Bell,

2005). To pinpoint the major causes of insecurity among the Apache HTTP servers deployed by Softetape's clients to the cloud, the author uses the following methods to gather data needed to identify and narrow down the root causes of the problem:

2.1 Document Analysis

Just like in any cyber security breaches, the company has documents that capture incidents of attack on its clients' cloud-based applications. These postmortem documents give the author an insight into what the potential threats could be. With these hypotheses in mind, the author uses the following two methods to narrow down the threats to a manageable size.

2.2 Survey and Interview

To provide an actionable recommendation and model implementation to Softetape's clients, a random number of clients were selected to answer a set of questions that will shed more light on the root cause of the problem. The questions were crafted in such a way as to make it easy to map to potential threat to a web server. The survey is made available in both hard copy as well as a web-based form. The hard copies were filled and returned immediately to the author. After receiving the link to the online version, they were filled and submitted through Surveymonkey (www.surveymonkey.com), an online form-as-a-service website. Some of the selected clients politely declined filling the form online or otherwise. The author was able to convince them to grant a short interview during which the author was able to ask the questions on the survey and extract the needed information.

2.3 Direct Observation

One of the questions on the survey asked the clients if they will be willing to participate in a direct observation exercise and some respondents agree to such an arrangement. The exercise entails tagging along a respondent while he or she configures and secures his or her Amazon web service EC2 instance or EC2 Docker container. The experiment also includes observing some members of the cloud consulting team giving on premise or remote support to some of the clients needing help in setting up or troubleshooting their cloud server.

3 Literature Review

This section examines in brief the theoretical background for this thesis. It also serves as a link between the theorem and the practical aspect of this project.

3.1 Cloud Computing

According to National institute of Standards and Technology (NIST), cloud computing is defined as:

"*A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*"

From the above definition, it is evident that cloud computing has some similarity with old computing concepts like hosted servers, grid computing and collocated data centers. However, there are key distinguishing factors that differentiate it from these concepts. These five essential characteristics are:

- On-demand self-service: this feature highlights the easy with which a consumer in need of computing resources from a cloud provider can provision such resources without the involvement of the provider support staff. For example, a web developer who wants to deploy a web server in the cloud either using virtual servers or Docker containers can spin one up from the Amazon Web Services Console after signing into his or her account without the involvement of Amazon support staff.
- Broad network access: cloud resources are acquired over the internet irrespective of the medium, transport protocols, interfaces or security technologies (Erl, Puttini and Mahmood, 2013). This simply means each consumer of a cloud resource should be able to interact with a cloud platform in ways that suit their needs or job roles. As an

example, a member of the DevOps team for a web development company can provision a cluster of Docker containers from his or her AWS mobile apps or from a browser on a personal computer for a programmer. The programmer will then use AWS RESTFUL API's in interacting with the aforementioned resources in his or her application.

- Resource pooling*:* this feature emphasizes the pool property of cloud resources. Cloud resources are offered to multiple consumers and each customer takes from the pool what he or she needs and releases them back when they are no more needed. This capability is enabled by virtualization technologies (Erl, Puttini and Mahmood, 2013).
- Rapid elasticity: With vast IT resources in its pool cloud provider can transparently provision for its consumers the resources they need when needed at a competitive rate.
- Measured Service: This refers to the capability of the cloud platform to gather data that is used for billing and other allied matters.

3.1.1 Cloud Delivery/Service Models

Cloud delivery model is a distinct suite of IT resources provided by a cloud provider (Erl, Puttini and Mahmood, 2013). These pre-packaged suites of resources are also a demarcation of the different responsibilities of both the cloud provider and the consumer. The common suites are:

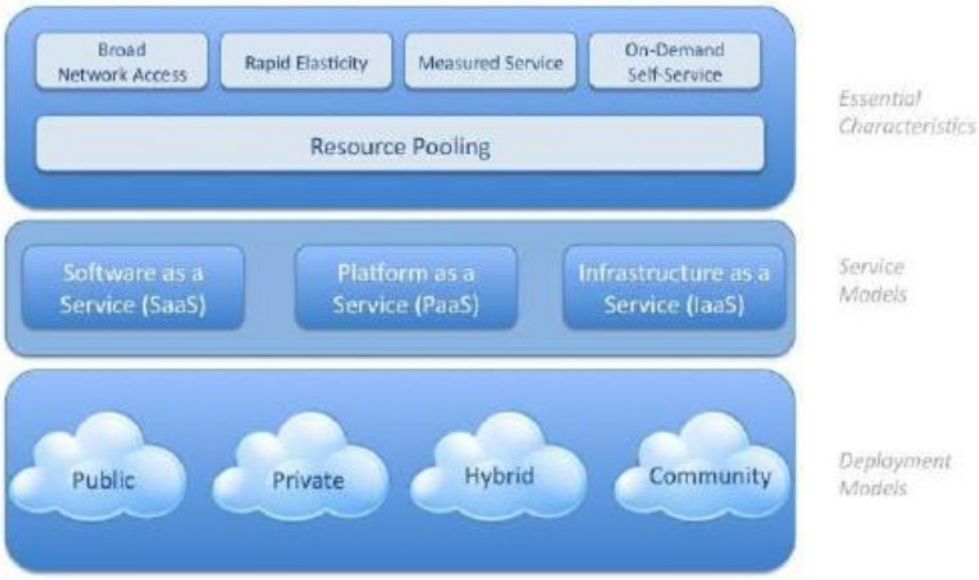
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

3.1.2 Cloud Deployment Models

A cloud deployment model classifies cloud environment mainly by its ownership, size and access. The four common classes and definitions are tabulated in the table below.

Public Cloud	This is a third-party cloud that is available to the general public
Community Cloud	A community cloud shares the same property of the public cloud except that its access is restricted to a certain group of cloud users
Private Cloud	This type is own and available to a single company
Hybrid Cloud	This type is a mixture of any of two or more models

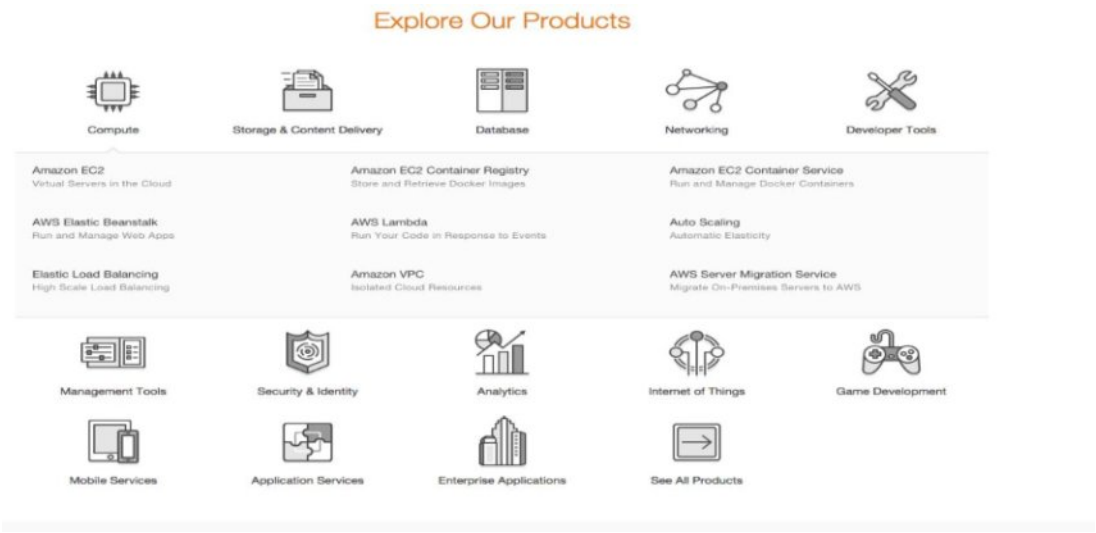
The relationship between the service models and the deployment models are depicted in the National Institute of Standards and Technology *Visual Model of Cloud* figure below.



Copied from nist.org

3.1.3 Amazon as a Cloud Provider

Amazon web service is a public cloud offering from Amazon Inc. in the United States. Its banquet of services covers the whole spectrum of the cloud service model and it is constant adding more to its services and categories. The figure below gives a point-in-time snapshot of its service offerings.



3.2 Web Server

For the purpose of this thesis, a web server is the software that resides on an (internet-enabled) computer hardware listening and responding to HTTP requests from clients like a browser (Laurie and Laurie, 2002). A web server can turn to an application server for a particular application type with the installation of appropriate plug-in or module to augment the capability of the web server. As an example, adding uWSGI module to the NginX web server extends its capability and enables it to process Python-based applications pages.

3.2.1 Popular Web Servers

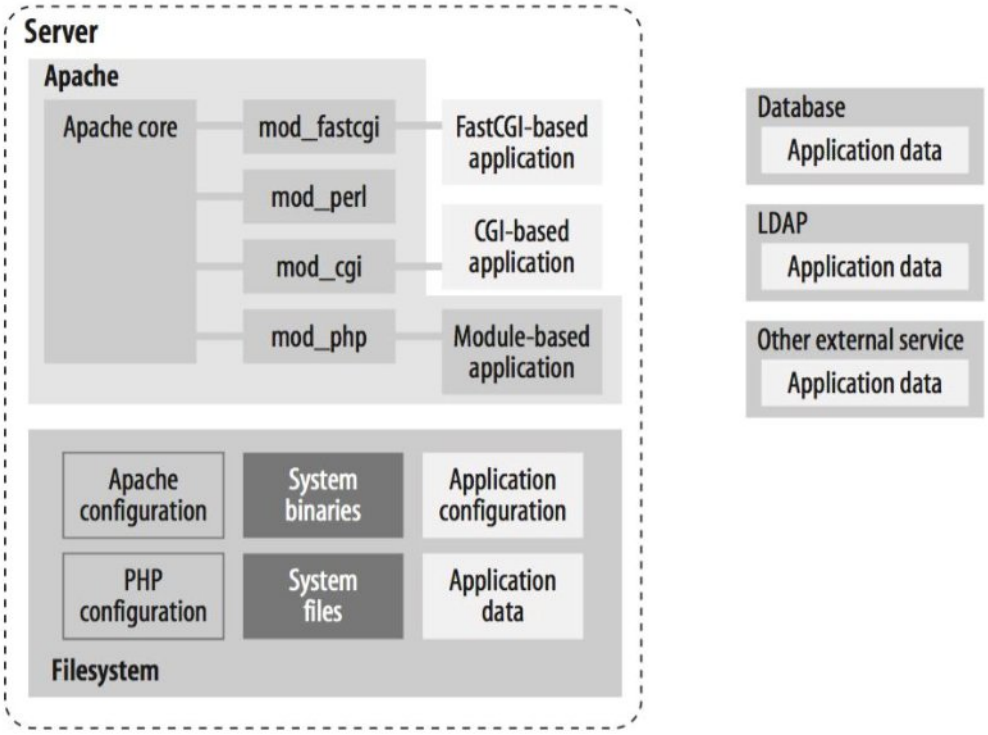
According to Netcraft February 2016 web server survey, there are four HTTP servers that are widely used on the internet. These HTTP servers account for about eighty per cent of the market share (news.netcraft.com, 2016). The table below tabulate their individual market share as at the aforementioned month above.

Developer	January 2016	Percent	February 2016	Percent	Change
Apache	304,271,061	33.56%	306,292,557	32.80%	-0.76
Microsoft	262,471,886	28.95%	278,593,041	29.83%	0.88
nginx	141,443,630	15.60%	137,459,391	14.72%	-0.88
Google	20,799,087	2.29%	20,640,058	2.21%	-0.08

(Copied from netcraft.com)

3.2.2 Apache Web Server Architecture

Securing Apache web server will be difficult without first understanding the different parts that make up the web server and how they relate to each other. Apache HTTP server is made up of a core component with additional modules to extend its capabilities. The figure below shows the different parts that makes up Apache web server:



Copied from “Apache Security”

3.3 Security Frameworks and Benchmark for the Project

In evaluating the security stance of the clients' web server and cloud accounts, the author uses the following security frameworks and benchmark as references:

- National Institute of Standards and Technology (NIST) Guidelines on Securing Public Web Servers (code named SP800-44)
- Centre for Internet Security (CIS) Apache HTTP Server 2.4 Benchmark
- Centre for Internet Security (CIS) Amazon Web Services Foundations Benchmark
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing
- European Union Agency for Network and Information Security (ENISA) Threat *Landscape 2015*

In view of the fact that the above frameworks provide a balance of both the theorem and practical knowledge for the subject matter of this thesis, the author would be recommending them to the customers as the first set of documents to peruse when deploying a web server to the cloud.

4 Threat Analysis

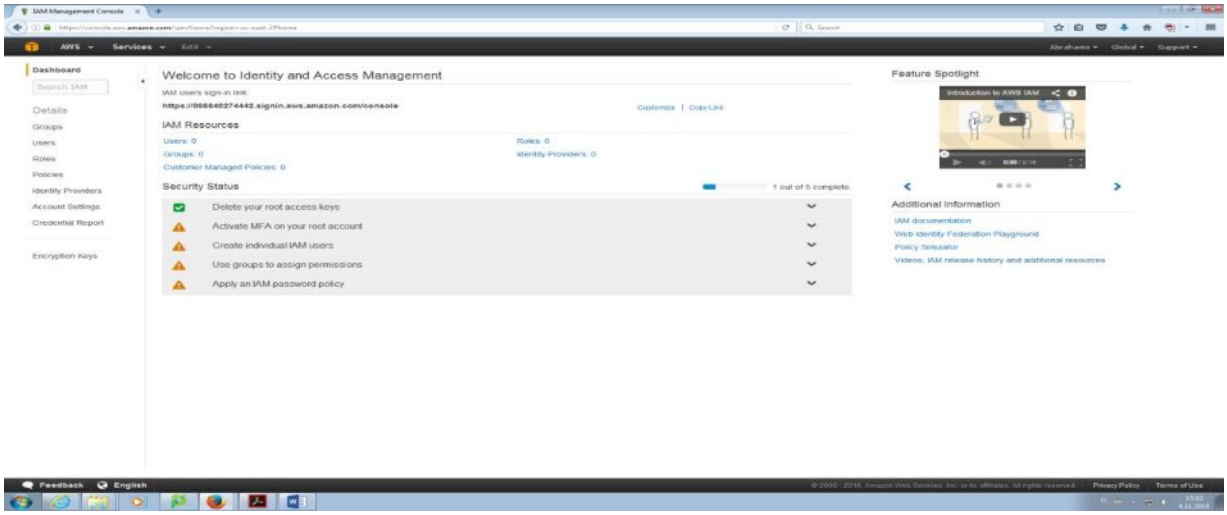
After analysing the data gathered from the company breach documents, clients' survey and interviews, the paragraphs below detail the problems discovered and appropriate mitigations.

4.1 Technical Issues and Recommendations

This section captures some of the prevalent technical issues affecting the customers' cloud security.

4.1.1 Amazon Identity and Access Management (IAM) Issues

For most of the clients having problems with their cloud accounts, it was discovered that they knowingly or unknowingly ignored the cloud provider's recommendations, which make them more vulnerable to attacks. The figure below show screen shot of Amazon recommendations.



For a secure access to the cloud management console, Amazon recommends that its customers should carry out the following tasks before putting its platform in production environment:

- Delete root access keys: this is done automatically for the customer. However, a user can still generate a new key if he or she so desires thus weakening the platform security.
- Activate multifactor authentication (MFA): MFA hardens the clients account security by requesting the user to provide an authentication code from an MFA device after they have given their user and password correctly.
- Create individual IAM users: As a security best practice, it is better to provide a client's employee with the least system privilege to do their job than create a single account that can be use by everybody. This not only promote security but makes monitoring and auditing possible.
- Use group to assign permissions: As a company grows, assigning privileges to each user becomes a tedious and boring task that can leave a loophole in the security of the platform. In addition, the cloud admin may assign too much privilege to a user more than they need to do their job. Using a group enable the admin to plan beforehand what groups are needed and what is the minimum privilege the members will need to do their job.
- Apply an IAM password policy: Without a policy like this, the users can weaken the security of the platform by using weak passwords or reusing old passwords.

4.1.2 Encryption Issues

Encryption is widely used by Amazon for securing its platform and the clients' data. It has also added many cryptographic features to almost all its platform services. While Amazon recommends that its customers encrypt their data both in transit and at rest, the author discovered that most of Softetape's customers are not using some of these features where they needed them the most. A common case is that of customers dumping their database SQL script to a publicly accessible Simple Storage Service (S3) buckets without encrypting it. The solution to problem like this is for the customers to be continually educated on available cryptographic features, when to use them and the right way to use them.

4.1.3 Key Management and Exchange Issues

Amazon platform admins or privilege users can generate both the public and private keys for a cloud user. Transmission of the private key is an issue to some of the customers especially where the staffs are geographical dispersed. It is also possible to import a user public key to the platform thus where the secure transmission of the private key can not be guaranteed or ascertained the users should be asked to generate its own key pairs and send the public key to the admin or the privileged user concerned.

4.1.4 Machine Image Misconfiguration

Some of the customers deployed their own private machine images or customised public images. The problem with these images are they all contain data or configurations that are dangerous in the hands of a malicious third party. To solve this problem, the support team will be providing machine images that can be downloaded and used by the customers since there is a bridge of trust between them and the customers. In addition, the customers should be educated on how to encrypt their machine images by the team.

4.1.5 Web Application Security

According to ENISA, web application security is part of the top emerging threat to the cloud. The figure below summaries ENISA list of emerging threat to the cloud:

	Emerging Threat	Threat Trend
1.	Malicious code	↑
2.	Web based attacks	↑
3.	Web application attacks	↑
4.	Botnets	↑
5.	Denial of Service	↑
6.	Insider threat	↑
7.	Data breaches	↑
8.	Cyber espionage	↑
9.	Identity Theft	↑
10.	Information leakage	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 4: Emerging threats and their trends in the area of cloud computing

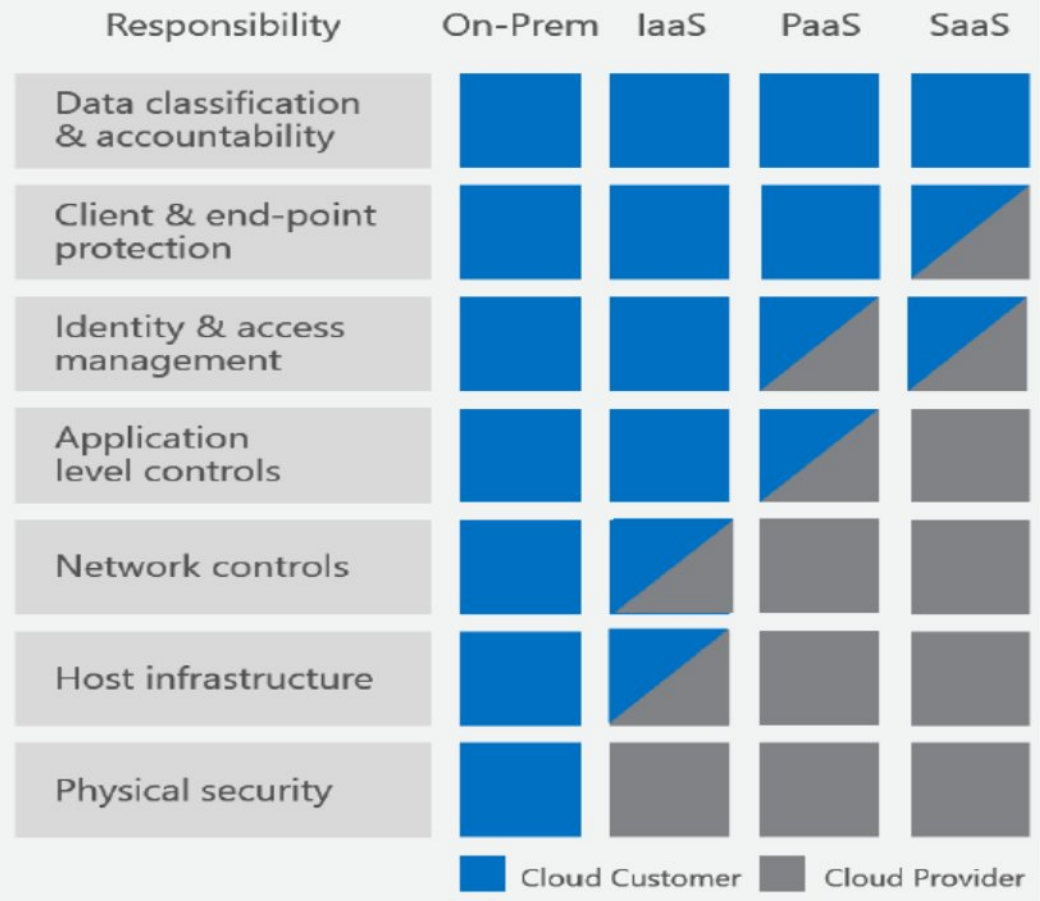
Copied from ENISA Treat Landscape 2015

While securing the cloud platform, the operating system and the web server increases security, it does not completely eliminate the security risk. Web application security also contributes its quarter to the woes of Softetape's clients. Eliminating buggy codes requires coders that are knowledgeable in secure software development. To this end, the author recommends to the support team to start a 'coders clinic' meet up that is focus on web application security and can be attended virtually. The customers have received this with open arms

4.2 Secondary Factors and Recommendations

4.2.1 Shared Responsibility Model

Shared responsibility model defines who is responsible for what at each layer of the cloud (Shinder, 2016).The service model chosen by the customer determines where a customer responsibility ends. After analysis, the author discovered that some of the customers bought the wrong service. In most cases, these customers subscribed for infrastructure-as-a-service (IaaS) model while what they will be able to manage is a platform-as-a-service (PaaS) model. The figure below shows the responsibility matrix depending on the service model adapted.



copied from blogs.msdn.microsoft.com

4.2.2 Multitier Risk Management

When deploying a web-based application to the cloud, the risk assessment should cover several level of the infrastructure such as the cloud platform, operating system, database management system, web server and the application. Most of the customers' assessment only cover two or three of the aforementioned level. This makes them vulnerable at the layers where they do not proactively assesse their exposure and implement measures to minimise or eliminate the risk.

4.2.3 Voluminous Documentation

Virtually all the customers complain about the difficult in finding the information they need from the official documentations at https://aws.amazon.com/documentation/. To ameliorate this problem the author worked with the support team in setting up a secure support portal that can be used by the customers in accessing well-written how-to articles as substitute for some part of the documentations. The customers can also send in request for assistant through the secure portal.

4.2.4 False Sense of Cloud Security

A mentality of anything cloud based is secure makes lot of organisations leave the pre-migration tasks undone (Doyle, 2016). This much is true for my client customers as the planning and the risk assessment stages for the cloud are carried out by a few. To reverse this

trend, the support team will need to be more involve at the planning and risk assessment stages.

5 Model Implementation

The purpose of the model implementation is to demonstrate the minimum security configurations that should be done to Amazon cloud platform, the EC2 instance as well as create a secure (harden) web server that could be used as a starting point by Softetape's clients when deploying their application in Amazon cloud.

5.1 Case Study

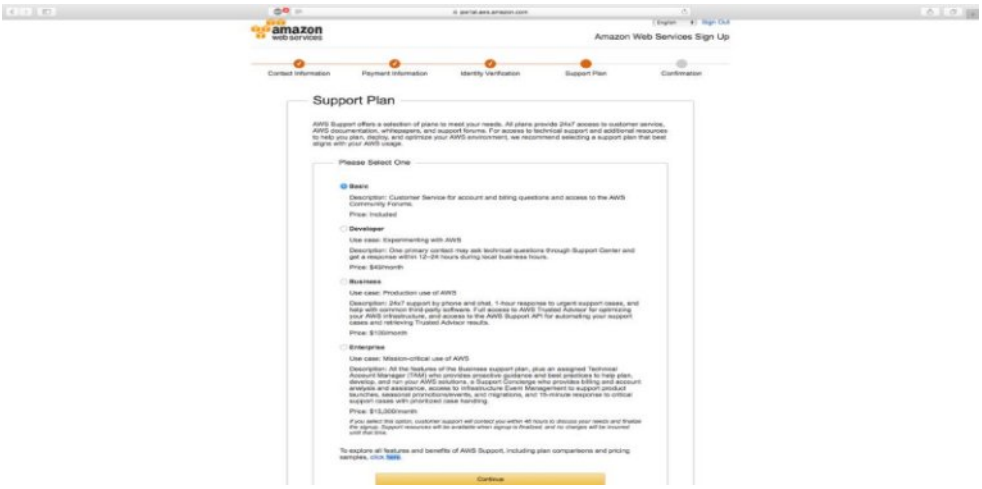
To give the model implementation context, the requirements of a new Softetape customer is used as a case study. ABC Ltd. (not real name) is deploying an automobile sales website to Amazon cloud. ABC limited will be competing with the likes of Cheki Nigeria Limited (https://www.cheki.com.ng/) and Jumia Nigeria Limited (http://car.jumia.com.ng/). Apart from the founder, ABC limited has three employees – two developers and one operations support staff.

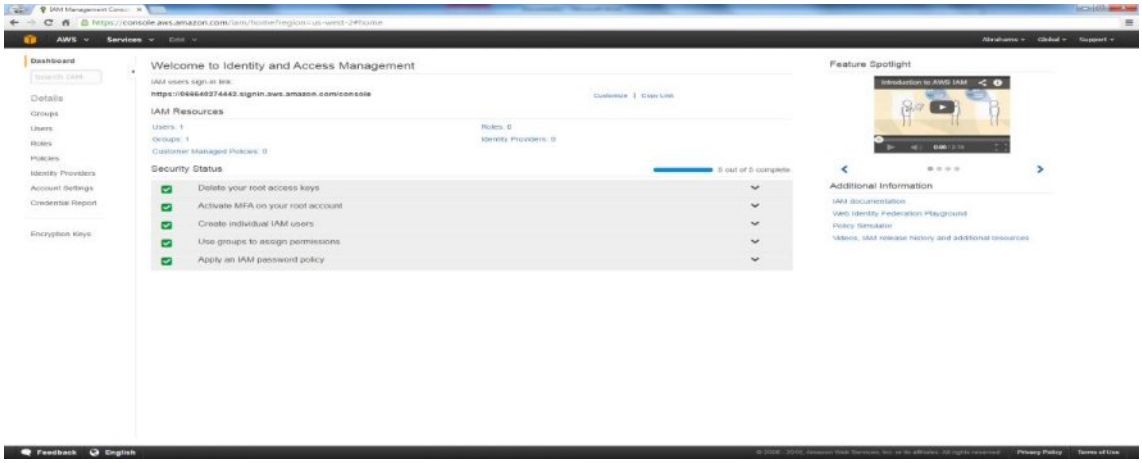
5.2 Securing the Cloud Environment

To strengthen the cloud platform security, Amazon recommends that the following minimum steps be followed to secure the platform (AWS Identity and Access Management User Guide, 2016).

5.2.1 Sign up for an account and enable AWS multifactor authentication (MFA)

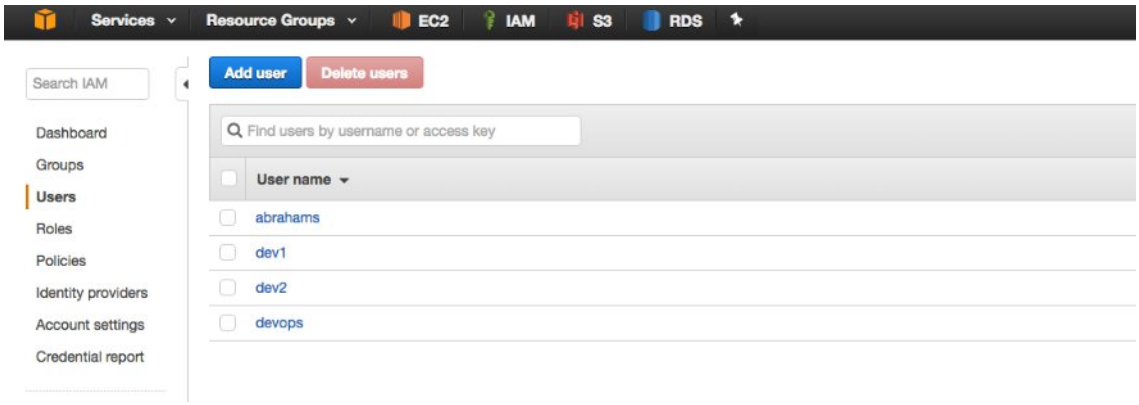
The first step is to sign up for an account on amazon website at https://aws.amazon.com/.To successfully create the profile, the founder uses his credit card, email address and phone number. The figures below show some of the snapshots while creating the account.





5.2.2 Create individual IAM users

In accordance with the principle of separation of duties, Amazon recommends that every employee that will be working with the platform should have his or her own user account.
For ABC limited, four accounts are created as shown in the figure below.



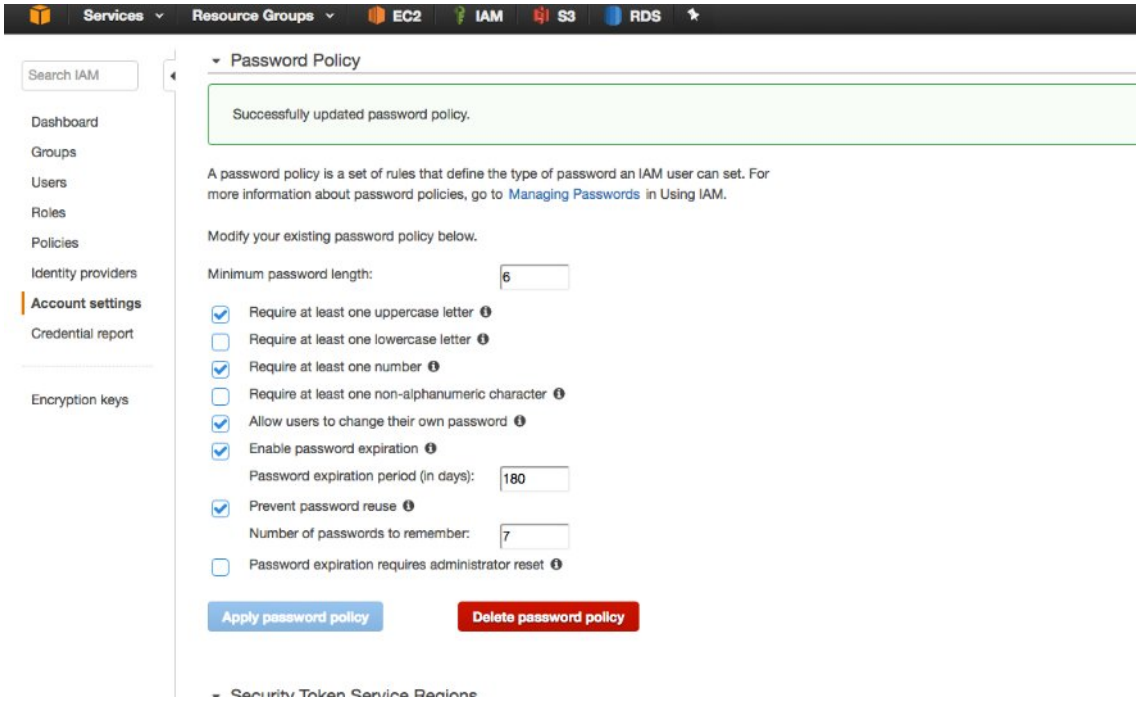
5.2.3 Create groups to assign permissions and give only the minimum privilege

AWS groups are collections of permission that can be assigned to multiple users.A user can be assigned multiple groups but groups can not be nested.

ABC limited cloud groups

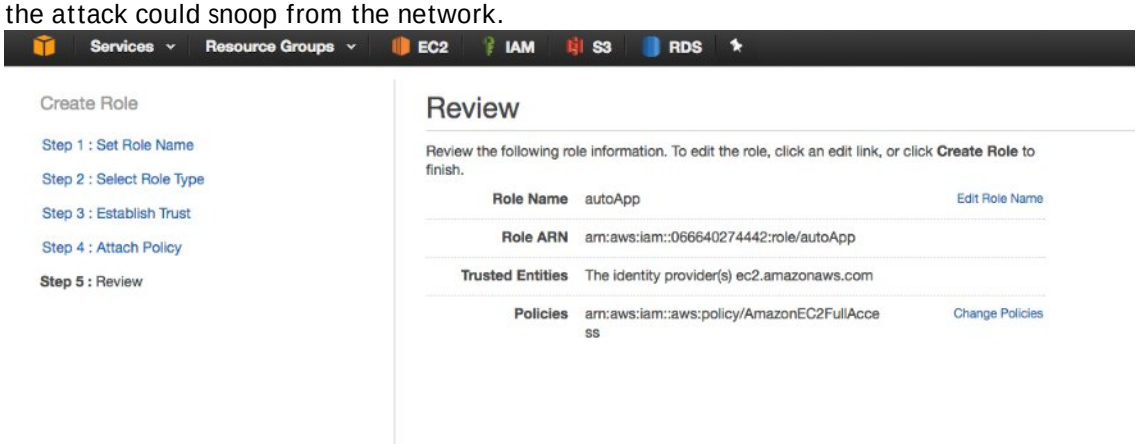
5.2.4 Configure password policy and enable MFA for privileged users

AWS privileged users can manage and administer the service from their browsers. An easy to guess password or a vulnerable one is a high security risk. AWS password policy helps in enforcing password complexity thus thwarting such an attack. Also enabling multifactor authentication for privileged users in addition to the root user will as well harden the the authentication and authorisation process. The figure below shows the password policy configured for ABC limited.



5.2.5 Create role for the Auto website

In Amazon cloud, giving permission to web application is a little different from that of a user. For an application to be able to connect to AWS resources, appropriate permissions must be assigned to a role, which is subsequently granted to the application. Using roles in AWS when granting access to application is securely better than embedding access keys that the attack could snoop from the network.



5.2.6 Enable CloudTrail

Every resource request to Amazon cloud is through its application programming interface (API). CloudTrail is a web service that provides a log of all calls made to the API. In order to be able to monitor how the cloud resource in being used and by whom, CloudTrail will be turned on.

5.3 Harden Apache Web Server

After other layers of the infrastructure have been harden,the apache web server needs to be secure too. Apache Software Foundation security home page recommends the following steps for toughening up the server (Httpd.apache.org, 2016) :

- Update Apache codebase regularly
- Tune Apache configuration to immunise it against Denial of Service (DoS) attacks
- Set appropriate permissions on ServerRoot Directories
- Protect Server Files by Default
- Monitor Apache log files
- Merge configuration sections

To complement Apache Software Foundation recommendations, the Centre for Internet Security Apache Benchmark guide are followed to the letter.

6 Conclusion

6.1 Presentation of findings and Model implementation

I have presented my findings and recommendations to some of the concerned clients and Softetape Cloud support team at company headquarters in Lagos on the 20th of December 2015. During my presentation, I highlighted keys issues affecting their cloud security as well as that of the web servers and gave a comprehensive recommendation than I can pen down in this dissertation. My presentation was well received by both the clients and support staff.

6.2 Suggestion for further Development

To round off this dissertation, I would like to make the following suggestions to the company's management in order to advance the result of this thesis:

- The company should commission other projects that will look into secure configuration of other web servers like Nginx and IIS being used by some of its other clients
- The coders' security clinics pioneer by this project should be made a regular event during which startups and programmers advanced their knowledge of secure coding
- GUI applications that the customers can use to generate appropriate AWS CLI commands for a given task they want to accomplish should be develop by the company and made available to them. This will reduce security loopholes due to misconfiguration.

References

Bell, J. (2005). Doing your Research Project. England: Open University Press.

Erl, T., Puttini, R. and Mahmood, Z. (2013). Cloud computing. New Jersey: Prentice Hall Pearson Education.

Marinos, L., Belmonte, A. and Rekleitis, E. (2015). ENISA Threat Landscape 2015. Accessed 11 July 2015.https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport.

Yin, R. K. (2009). Case Study Research Design and Methods. California: SAGE Publications Inc.
Laurie, B. and Laurie, P. (2002). Apache the Definitive Guide. O'Reilly.

W3techs.com. (2015). Usage Statistics and Market Share of Web Servers for Websites for November 2015. Accessed 25 Nov. 2015.
https://w3techs.com/technologies/overview/web_server/all.

AWS Identity and Access Management User Guide. (2016). Amazon Web Services, Inc. Accessed 3 Jan. 2016.
https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwilt-bXb5a_QAhWIESwKHTM8C9AQFggkMAA&url=http%3A%2F%2Fdocs.aws.amazon.com%2FIAM%2Flatest%2FUserGuide%2Fiam-ug.pdf&usg=AFQjCNHCh_eFSe2TCh4pNoGjDw4l8vk-uQ

Shinder, T. (2016). What does shared responsibility in the cloud mean?. Accessed 22 Apr. 2016. https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

Amazon Elastic Compute Cloud - User Guide for Linux Instances. (2016). Amazon Web Services, Inc. Accessed 3 Jan.2016 .
https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&sqi=2&ved=0ahUKEwjN_vLS9q_QAhWHfywKHX7KAggQFgg4MAE&url=https%3A%2F%2Fdocs.aws.amazon.com%2FAWSEC2%2Flatest%2FUserGuide%2Fec2-ug.pdf&usg=AFQjCNFWnJMCLcxk8kR1LGt354r-NPpyTQ&bvm=bv.139138859,d.bGg

Wainwright, P. (2004). Pro apache. Berkeley, Calif.: Apress.

News.netcraft.com. (2016). February 2016 Web Server Survey | Netcraft. Accessed 25 Feb. 2016.
https://news.netcraft.com/archives/2016/02/22/february-2016-web-server-survey.html

National Institute of Standards and Technology (NIST), (2016). NIST's Visual Model of Cloud Computing Definition. Accessed 7 Mar. 2016. http://www.security-daily.com/dsp_getFeaturesDetails.cfm?CID=2651

Guidelines on Securing Public Web Servers. (2007). National Institute of Standards and Technology, pp.51-52,128-136. Accessed 2 Apr. 2016.
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

Durkee, R. (2016). CIS Apache HTTP Server 2.2 Benchmark v3.4.0. Accessed 10 Jun. 2016.
https://benchmarks.cisecurity.org/downloads/show-single/index.cfm?file=apache.340

Montville, A., Spiess, C., Frantz, B., Fitzpatrick, G., Rodriguez, I., Pathak, A., Covington, J., Launey, C., Witoff, R., Martinez, J., Sandage, T., de Libero, M. and Corley, A. (2016). CIS

Amazon Web Services Foundations Benchmark v1.0.0. Accessed 4 Jan. 2016. https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

Doyle, J. (2016). Cloud – a false sense of insecurity? Accessed 14 Nov. 2016. http://www.annodata.co.uk/blog/cloud-a-false-sense-of-insecurity/
Httpd.apache.org. (2016). Security Tips - Apache HTTP Server Version 2.4. Accessed 25 Nov. 2016. http://httpd.apache.org/docs/2.4/misc/security_tips.html